Opportunités et risques du numérique pour le citoyen usager des services publics

Degrave, Élise

Published in:
Vulnérabilités et droits dans l'environnement numérique

Publication date:
2018

Document Version
le PDF de l'éditeur

CHAPITRE 14
Opportunités et risques du numérique pour le citoyen usager des services publics

Elise DEGRAVE[1]

Toute sa vie durant, le citoyen est contraint de se dévoiler à l'État, en lui communiquant ses informations les plus personnelles. Cela commence à sa naissance, par l'enregistrement de ses données d'identification au Registre national et la communication de son existence à l'organisme chargé du paiement des allocations familiales. Plus tard, son parcours scolaire sera tracé tout comme l'évolution de sa santé, ses données de carrière, de pension, sa situation maritale, la composition de sa famille, ses déménagements successifs, etc.

En somme, durant sa vie entière, ses contacts avec les services publics seront nourris de quantités de données à caractère personnel qu'il n'a pas le choix de communiquer, au risque d'agir au mépris de la loi voire, de ne pas avoir d'existence civique.

La communication et l'utilisation de ces informations soulève des enjeux nouveaux à l'ère numérique. Pour le dire autrement, le citoyen, qui ne peut pas refuser de donner ses informations, n'a d'autre choix que de faire confiance à l'État dans la gestion de celles-ci. Et cette confiance est de taille : les données divulguées sont nombreuses et touchent à l'ensemble des aspects de sa vie quotidienne.

Pourtant, à l'heure du déploiement technologique, la confiance du citoyen en l'État a de quoi être ébranlée à maints égards. En effet, depuis plusieurs années déjà, l'usage des technologies provoque des bouleversements majeurs au sein des services publics, tant dans leur structure que dans leur fonctionnement. Nous sommes entrés pleinement dans l'ère de l'administration électronique, dite aussi l'ère de l'« e-gouvernement ».

De toute évidence, le numérique est une opportunité pour le citoyen, qui voit sa relation avec l'administration considérablement simplifiée à la faveur des technologies. Néanmoins, corollairement à ces avantages, des risques émergent, principalement s'agissant de la transparence des pratiques administratives dans l'e-gouvernement, et du contrôle de celles-ci.

[1] Chargée de cours à l'Université de Namur, chercheuse au Crids.

SECTION 1. – L'administration électronique : une opportunité grâce à la simplification administrative

§ 1. Le citoyen au cœur de la transformation de l'administration

1. La collecte unique des données. La transformation de notre modèle d'administration est pensée notamment par rapport au souci de simplifier la relation que le citoyen entretient avec l'administration.

Ces réflexions se fondent sur une première évidence : au cours d'une vie, le citoyen est contraint de fournir, de manière récurrente, les mêmes informations à des autorités distinctes. On songe notamment à l'adresse, la date de naissance, la composition de la famille, etc.

Par ailleurs, on ne peut ignorer que les technologies permettent l'échange aisé et la réutilisation infinie d'informations.

Ces deux constats conjugués ont abouti à la consécration d'un principe qui fonde aujourd'hui l'e-gouvernement belge : le principe de la collecte unique des données. C'est l'idée que le citoyen ne doit donner qu'une seule fois ses informations à l'administration à charge, ensuite, pour les différentes autorités publiques, de s'échanger ces informations entre elles lorsqu'elles en ont besoin.

La collecte unique des données n'est pas qu'un vœu pieu. Elle est concrétisée par l'obligation, imposée aux administrations, de collecter indirectement les données, via le réseau sectoriel plutôt qu'en les demandant directement aux personnes concernées. Nous y reviendrons.

2. Le concept de « *privacy by design* ». Le « *privacy by design* », ou « protection des données dès la conception » est un concept apparu dans les années nonante au Canada, grâce au travail de Ann Cavoukian, commissaire à la protection de la vie privée de l'Ontario[2]. Il est passé récemment sous le feu des projecteurs, lors de l'entrée en application du Règlement général sur la protection des données (RGPD) qui y consacre son article 25[3]. Il s'agit, pour le responsable de traitement, d'intégrer la protection de la vie privée en amont, dans la conception-même du sys-

[2] Ann Cavoukian y consacre un site internet (www.privacybydesign.ca). Voy. not. A. CAVOUKIAN, *Privacy by design…take the Challenge,* s.l., 2009.

[3] Cette disposition affirme notamment que « le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection

tème, plutôt que de créer ce système et de penser seulement ensuite à protéger la vie privée par des normes[4]. Pour le dire autrement, il s'agit de créer des outils qui, en eux-mêmes, présentent des garanties de protection pour la vie privée des personnes concernées. De cette manière, la protection de la vie privée est soutenue par la technique, en sus d'être organisée par des normes. Ensemble, ils constituent « un rempart efficace contre les excès rendus possibles par le progrès »[5].

Bien avant le RGPD, le « *privacy by design* » a reçu un ancrage concret en droit belge, au moment de poser les premières pierres de notre modèle d'administration électronique. Ce modèle a été conçu dans le souci de protéger la vie privée dès la mise en place des outils. En effet, les données des citoyens étant traitées massivement par l'État, l'on a renoncé à regrouper celles-ci au sein d'une grande base de données. Une telle centralisation aurait été trop risquée au regard des risques de piratages informatiques notamment. Dès lors, le choix a été fait d'organiser une décentralisation des données, à savoir, la dispersion des données entre plusieurs bases de données et la mise en place d'outils permettant l'échange de données sécurisé entre les différentes administrations. C'est le modèle que nous expliquons dans les lignes qui suivent.

§ 2. L'administration électronique en Belgique : un modèle inédit

3. De l'administration en silos à l'administration en réseaux. Longtemps, l'administration était structurée en silos. Les institutions publiques œuvraient de manière cloisonnée, collectaient auprès des citoyens les informations dont elles avaient besoin pour l'exécution de leurs propres missions et ne les partageaient pas ensuite. Il en résultait une perte de temps et d'argent pour l'administration, qui devait contacter chaque personne pour chaque information nécessaire, attendre sa réponse, réclamer éventuellement des précisions, mais aussi pour le citoyen qui était contraint de communiquer de multiples fois la même

---

des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée ».

[4] J. Le Clainche, « Consentement et traitements de données à caractère personnel », in *Les technologies de l'information au service des droits : opportunités, défis, limites* (D. Le Métayer dir.), Bruxelles, Bruylant, 2010, pp. 166 à 169 ; M. Groothuis, « De digitale overheid en de menselijke maat », *Computerrecht,* 2009, p. 240.

[5] J. Le Clainche, « Consentement et traitements de données à caractère personnel », *op. cit.,* p. 168.

information aux institutions gérant un dossier à son sujet, d'effectuer des démarches administratives qui impliquaient d'identifier l'administration compétente, de se déplacer, de respecter des horaires stricts et de prendre patience dans les files d'attente.

Avec l'apparition des technologies, on constate que les administrations peuvent désormais collaborer efficacement. La volonté naît alors d'encourager les « synergies entre les divers services et niveaux des pouvoirs publics »[6], dans le but de simplifier les démarches et procédures administratives. La technologie rend aisé et rapide l'échange des informations relatives aux citoyens. Cela permet notamment d'alléger les tâches administratives des citoyens, en automatisant l'octroi de certaines allocations, par exemple, et de renforcer l'efficacité de l'administration, en améliorant la lutte contre la fraude, notamment[7].

Pour mettre en œuvre efficacement l'échange des informations entre administrations, la Belgique s'engage, depuis plusieurs années, dans un modèle d'administration tout à fait inédit, qui consiste à mettre en place des réseaux d'administrations au sein desquels un intégrateur de services assure l'échange des données entre les administrations concernées.

Plus précisément, dans un premier temps, les administrations ayant un point commun (par exemple, un objet de travail commun ou l'appartenance à une même entité, fédérale ou fédérée) sont regroupées au sein d'un ensemble appelé « réseau ».

Ensuite, différentes administrations se voient attribuer la responsabilité de collecter, enregistrer et mettre à jour certaines données déterminées. Les bases de données contenant ces informations et placées chacune sous la responsabilité d'une administration sont appelées « sources authentiques de données ». L'idée est de faire en sorte que chaque information relative au citoyen ne soit enregistrée qu'une seule fois par une seule administration du réseau, qui est ensuite responsable de la fiabilité de ces données.

Enfin, on place, au cœur de ce réseau d'administrations, un outil d'un type nouveau : l'intégrateur de services, dit aussi « plateforme d'échange d'informations » ou encore « banque-carrefour ». En somme, l'intégrateur

[6] Commission de la protection de la vie privée (ci-après « CPVP »), avis n° 41/2008 du 17 décembre 2008 relatif à une demande d'avis concernant l'avant-projet de loi relative à l'institution et à l'organisation d'un Intégrateur de services fédéral, n° 5.

[7] Pour de plus amples développements sur l'e-gouvernement et le modèle de l'administration en réseaux, voy. D. De Bot, *Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart als belangrijkste juridische bouwstenen*, Bruges, Vanden Broele, 2005, pp. 1 à 13 ; E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, coll. Crids, Bruxelles, Larcier, 2014, en particulier n^{os} 172 et s.

de services est une infrastructure technique, placée au cœur d'un réseau d'administrations, et qui est chargée d'assurer, au sein de ce réseau, l'échange électronique d'informations provenant de sources authentiques diverses. Ainsi, lorsqu'une administration a besoin d'une donnée dont elle ne dispose pas, il lui suffit de s'adresser à l'intégrateur de services qui contacte l'administration détentrice de la donnée recherchée et l'achemine ensuite vers l'administration qui la lui a demandée.

Afin de faciliter la compréhension de l'exposé, on peut, d'ores et déjà, schématiser comme suit le modèle d'un réseau d'administrations comprenant un intégrateur de services.

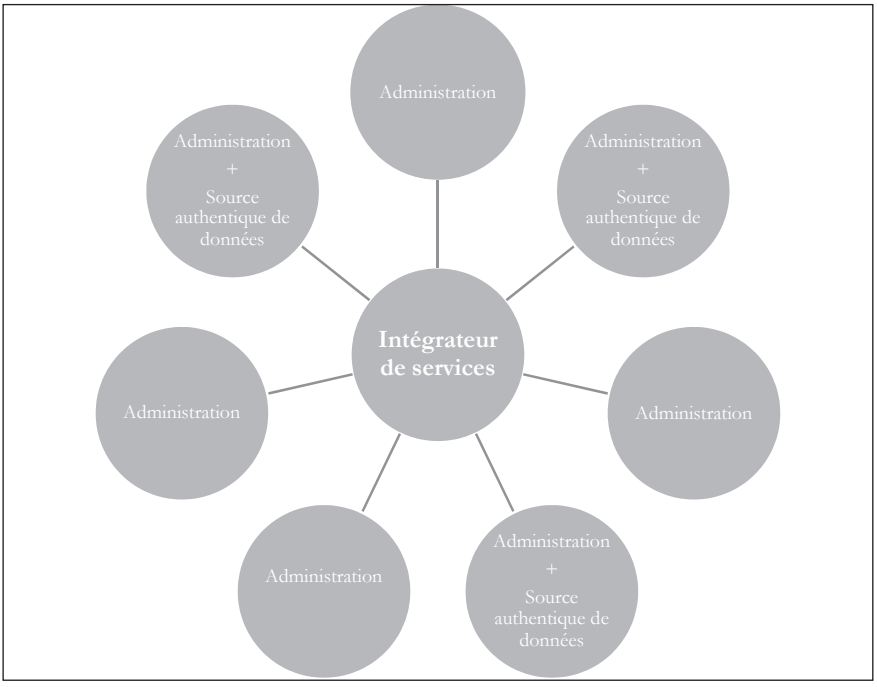
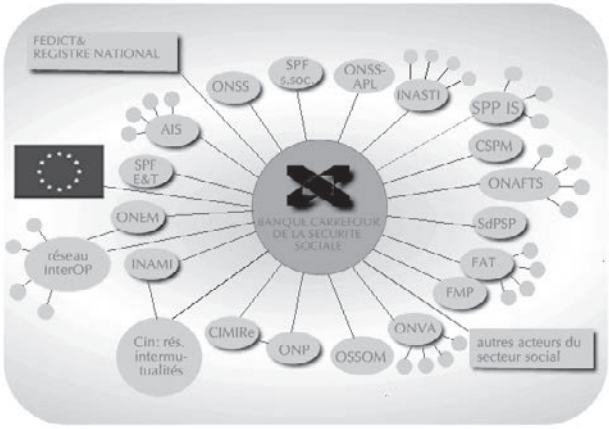


Schéma illustrant un réseau d'administrations composé d'un intégrateur de services auquel sont reliées plusieurs administrations dont certaines détiennent une source authentique de données.

Depuis quelques années, plusieurs réseaux d'administrations ont progressivement été créés au sein du secteur public belge. Ils comprennent chacun, en leur cœur, un intégrateur de services. Historiquement, le premier réseau du genre est le réseau de la sécurité sociale, qui regroupe les institutions de sécurité sociale et au sein duquel œuvre la Banque-carrefour

de la sécurité sociale. Ce réseau et cet intégrateur de services sont en place depuis le début des années nonante[8]. Depuis lors sont apparus d'autres réseaux, tels que notamment le réseau sectoriel de la santé, au sein duquel la plate-forme *eHealth* assume le rôle d'intégrateur de services[9] ou le réseau des véhicules avec en son cœur la Banque-carrefour des véhicules[10].



Exemple d'intégrateur de services vertical : la Banque-carrefour de la sécurité sociale, placée au cœur du réseau de la sécurité sociale

4. Opportunités pour l'administration et pour le citoyen. De toute évidence, l'efficacité de l'administration est renforcée grâce à l'échange rapide d'informations exactes et à jour. Le citoyen voit également ses tâches facilitées. Il peut accéder à nombre d'informations en ligne et effectuer des transactions administratives à tout moment depuis son ordinateur. Il est également épargné de certaines démarches administratives grâce à l'automatisation des procédures. À cet égard, par exemple, une application informatique créée par l'intégrateur de services fédéral et dénommée *Ebirth* facilite l'échange des données relatives à la naissance d'un enfant. Ce service part du constat que tant les communes que la Communauté française et le SPF Economie ont besoin d'informations relatives à chaque naissance. Jadis, ces administrations obtenaient ces informations via des

[8] Voy. la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, *M.B.*, 22 février 1990. Ci-après « loi du 15 janvier 1990 relative à la Banque-carrefour de la sécurité sociale ».

[9] Voy. la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions, *M.B.*, 13 octobre 2008.

[10] Loi du 19 mai 2010 portant sur la création de la Banque-Carrefour des Véhicules.

formulaires en papier envoyés par les hôpitaux. Aujourd'hui, les hôpitaux se connectent au portail *Ebirth*, encodent les données requises, et celles-ci sont acheminées respectivement vers les communes, la Communauté française et le SPF Economie[11].

Progressivement, les portails de simplification administrative se multiplient, comme en témoigne le site www.mybelgium.be. On y trouve le lien vers différentes applications de service public, tels que tax-on-web (déclaration fiscale en ligne), mypension (calcul de la pension), mycareer (aperçu détaillé de la carrière), myminfin (dossier fiscal en ligne), etc., qui sont tous opérationnels.

§ 3. L'obligation légale de collecte indirecte des données et ses conséquences en jurisprudence

5. L'obligation de collecte indirecte des données. Ainsi qu'on l'a dit, le principe de la collecte unique des données a inspiré le modèle d'administrations en réseaux développé en Belgique. Ce principe n'est pas qu'un vœu pieux. Il est concrétisé par l'obligation, imposée aux administrations, de collecter indirectement les données, c'est-à-dire, d'obtenir les données des citoyens[12] en les demandant à l'intégrateur de services et non aux citoyens eux-mêmes. Plus précisément, cela signifie que ces administrations ne peuvent plus demander aux citoyens des documents qu'elles sont en mesure d'obtenir en s'adressant à l'intégrateur de services. Plus encore, elles ne peuvent plus exiger des citoyens qu'ils avertissent chaque administration d'une mise à jour de leurs informations si cette mise à jour est disponible dans une base de données du réseau sectoriel et qu'elles peuvent y avoir accès via l'intégrateur de services.

Le non-respect de l'obligation de collecte indirecte des données a des conséquences en pratique. Si une administration du réseau fédéral collecte directement auprès du citoyen une information qu'elle aurait dû obtenir via l'intégrateur de services, elle agit en violation de la loi. On doit alors considérer que les données relatives aux personnes concernées ont été obtenues illégalement, ce qui vicie la décision administrative prise sur la base de ces données. Dans le même sens, une administration ne peut plus refuser l'octroi d'un droit à un citoyen au seul motif qu'il ne lui a pas communiqué une information nécessaire, si celle-ci est disponible dans le

[11] Pour plus d'informations sur *Ebirth,* voy. la présentation générale d'*Ebirth* disponible à l'adresse https://www.ehealth.fgov.be/fr/esante/professionnels-de-la-sante/ebirth.

[12] Précisions que l'obligation de collecte indirecte des données s'applique également aux administrations qui traitent les données des entreprises.

réseau fédéral et que ladite administration peut y accéder via l'intégrateur de services.

6. Illustrations jurisprudentielles dans le secteur de la sécurité sociale. Ainsi qu'on l'a évoqué précédemment, une obligation légale de collecte indirecte s'impose depuis plusieurs années aux institutions de sécurité sociale pour les données disponibles dans le réseau de la sécurité sociale et accessibles via la Banque-carrefour de la sécurité sociale. Dans ce domaine, des décisions judiciaires existent, qui sanctionnent le non-respect de cette obligation. Elles sont encore rares mais s'avèrent particulièrement pertinentes.

Ainsi, par exemple, un arrêt rendu par la Cour du travail de Bruxelles, le 21 avril 2010[13], illustre le fait que l'obligation de collecte indirecte aboutit à contraindre les institutions de sécurité sociale à trouver par elles-mêmes les documents dont elles ont besoin dans l'exécution de leurs missions. C'est particulièrement intéressant, par exemple, pour un demandeur du revenu d'intégration sociale à qui le CPAS réclamerait un document que ce demandeur n'est pas en mesure de fournir alors que les informations recherchées sont disponibles dans le réseau de la sécurité sociale et que le CPAS peut y accéder. Dans un tel cas, malgré le fait qu'il n'a pas fourni ledit document, ce demandeur d'allocation ne peut pas se voir reprocher un manque de collaboration au sens de l'article 19, § 2, de la loi concernant le droit à l'intégration sociale[14] qui amènerait le CPAS à refuser l'octroi du revenu d'intégration sociale à cet assuré social. Le CPAS a, en effet, l'obligation de recueillir d'initiative les documents accessibles via la Banque-carrefour de la sécurité sociale[15].

D'autres décisions judiciaires rappellent que, par application de l'obligation de collecte indirecte des données, les institutions de sécurité sociale doivent veiller elles-mêmes à utiliser des données à jour, dès le moment où celles-ci sont disponibles dans le réseau de la sécurité sociale. La Cour du travail de Liège, par exemple, a rendu un arrêt à ce sujet le 27 juin 2006, en matière de droit à la pension[16]. Dans cette affaire, l'Office national des pensions[17] reproche à un homme pensionné de ne pas l'avoir averti du décès de son épouse, ce qui a des conséquences au niveau du montant de la pension qui lui est due. L'O.N.P. souhaitait récupérer le montant de pension trop élevé qu'elle avait payé durant cinq ans, en

[13] C. trav. Bruxelles (8e ch.), 21 avril 2010, R.G. n° 2008/AB/51591 et n° 2009/AB/51809.
[14] Loi du 26 mai 2002 concernant le droit à l'intégration sociale, *M.B.,* 31 mai 2002.
[15] C. trav. Bruxelles (8e ch.), 21 avril 2010, préc., 6e feuillet.
[16] C. trav. Liège, 27 juin 2006, *J.L.M.B.,* 2007, pp. 1043-1047.
[17] Ci-après « O.N.P. ».

invoquant les règles de prescription applicables en cas de mauvaise foi de l'assuré. Or, il s'avère que l'assuré social avait averti la commune du décès de son épouse. Cette information était donc enregistrée au Registre national, qui fait partie du réseau de la sécurité sociale. L'O.N.P., lui aussi inclus dans le réseau de la sécurité sociale, avait donc accès à cette information par l'intermédiaire de la Banque-carrefour de la sécurité sociale.

Compte tenu de ces éléments de fait et de droit, la Cour affirme qu' « un assuré social ne peut se voir imposer personnellement une obligation qui doit déjà être légalement remplie par une institution dont c'est la mission. C'est donc à tort que l'O.N.P. soutient que l'information transmise par la Banque-carrefour doit être doublée par une information émanant de l'assuré social et que seule celle-ci permettrait au pensionné de remplir ses obligations envers lui »[18].

En d'autres termes, dès le moment où l'assuré social communique à sa commune la mise à jour d'une information enregistrée au Registre national, il n'est plus contraint d'avertir les institutions de sécurité sociale de ce changement. C'est à ces dernières qu'il revient de mettre à jour les informations sur lesquelles elles fondent leurs prestations et ce d'autant plus que, le plus souvent, ces mises à jour leur parviennent automatiquement.

7. Une nécessaire modification des habitudes administratives en faveur des usagers du service public. L'obligation de collecte indirecte des données contraint les administrations à utiliser les outils technologiques à leur disposition et, ce faisant, à modifier leurs habitudes. C'est l'idée que « pour concrétiser les objectifs [de l'obligation de collecte indirecte des données], un changement de mentalité est nécessaire de la part des administrations. Redemander constamment des attestations aux citoyens et aux entreprises est une pratique courante. Cette méthode devra céder la place à une volonté de prendre soi-même l'initiative d'aller chercher les données nécessaires auprès des sources authentiques »[19]. À défaut de le faire, l'administration risquerait d'adopter des décisions illégales qui ne pourraient être appliquées.

À notre sens, l'obligation de collecte indirecte et la responsabilisation des administrations qui s'en suit est légitime. Elle répond à une volonté forte du législateur, affirmée dès les années nonante déjà[20], que la simpli-

[18] C. trav. Liège, 27 juin 2006, préc., p. 1047.

[19] Intervention de Peter Vanvelthoven, Projet de loi garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papiers, Ch. repr., sess. 2013-2014, n° 53-3387/004, p. 7.

[20] Entre autres exemples, voy. les travaux préparatoires de la loi du 15 janvier 1990 relative à la Banque-carrefour de la sécurité sociale, en particulier l'exposé des motifs, *Pasin.,*

fication administrative bénéficie tant aux administrations qu'aux citoyens et aux entreprises. Tous doivent gagner en confort grâce à l'informatisation des tâches administratives.

Dans le même temps, l'obligation de collecte indirecte des données et les sanctions applicables en cas de non-respect de celle-ci répondent à un but légitime dans notre société démocratique, celui de veiller à un certain équilibre entre l'administration et le citoyen[21]. En effet, grâce à l'intégrateur de services, l'administration gagne en efficacité et en confort dans l'accomplissement de son travail. Cela se fait en contraignant le citoyen à accepter que l'administration s'ingère à de multiples reprises dans sa vie privée en traitant ses données à caractère personnel. Il est légitime que ce citoyen ait un retour bénéfique direct du système mis en place, afin d'assurer une réciprocité des avantages de la technologie entre l'administration et le citoyen.

SECTION 2. – L'administration électronique : un risque créé par l'opacité du système

8. La disparition des dossiers papiers des citoyens. Certes, l'administration électronique permet d'alléger les démarches administratives des citoyens, grâce à la collecte unique des données et à l'obligation corollaire de collecte indirecte imposée aux administrations, ainsi qu'aux outils, de plus en plus nombreux, de simplification administrative.

Il n'en demeure pas moins que ce système aboutit à faire disparaître les dossiers papiers des citoyens. Non seulement, il n'y a plus de trace, sur papier, des données utilisées et des démarches effectuées, puisque de plus en plus d'informations et de démarches sont numérisées. Mais, surtout, le citoyen n'a plus de dossier accessible à un endroit unique, étant donné que ses données sont dispersées entre plusieurs réseaux sectoriels et, au sein de ceux-ci, entre plusieurs bases de données.

Ch. repr., sess. 1988-1989, n° 899/1, p. 77 : « la première mission de la Banque-carrefour (la transformation des flux d'informations actuels, désordonnés et éparpillés sur support papier, en flux électroniques coordonnés et harmonisés) doit permettre de réduire pour les personnes physiques et morales intéressées les charges ou obligations, le travail découlant d'une collecte de données qui est loin d'être caractérisée par l'unicité, de réduire les coûts administratifs de fonctionnement, les coûts sociaux dus aux cumuls indus non dépistés et d'accélérer le service rendu ».

[21] Pour de plus amples développements à ce sujet, voy. E. DEGRAVE, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, n° 47 à 49.

En d'autres termes, le citoyen ne sait plus qui détient ses données, qui les utilise, pour quelles raisons, quelles sont les données utilisées pour prendre telle décision ni si les données utilisées sont exactes et à jour.

§ 1. L'impératif de transparence

9. Voir et comprendre. Ainsi, l'usager de service public se trouve dans une situation de vulnérabilité, se sentant désormais perdu par rapport aux outils numériques complexes et opaques qui fondent l'administration électronique. Certes, certaines démarches administratives sont allégées voire automatisées et le citoyen est moins sollicité s'agissant de la communication de ses informations et de documents divers. Mais, en général, il ne voit plus, au sens propre, le cheminement des décisions administratives qui le concernent, et il ne comprend plus, ou si peu, sur quelles informations ces décisions sont fondées.

En somme, jusqu'à présent, il semble que l'on a surtout pensé le modèle d'administration électronique par rapport à l'efficacité que l'on peut tirer des technologies et l'on a mis en place des outils qui améliorent le travail des administrations, au bénéfice de ses usagers. Mais on a probablement perdu le citoyen en chemin, qui ne comprend plus les coulisses du travail de l'administration et, dès lors, n'est plus en mesure de contrôler celui-ci. Ce constat ne peut perdurer dans une société démocratique. C'est l'idée que « *within a democracy, citizen should not be left as pedestrians when the authorities drive limousines* »[22].

En particulier, l'impératif de transparence, fondé sur des justifications constitutionnelles et légales, doit accompagner le développement de l'administration électronique, pour plusieurs raisons.

Il s'agit, tout d'abord, d'un corollaire au *droit fondamental à la protection de la vie privée* des citoyens. Le droit fondamental à la vie privée, consacré par l'article 22 de la Constitution, s'entend aujourd'hui d'un droit à l'autodétermination informationnelle. En d'autres termes, chacun a le droit de décider lui-même de l'utilisation de ses données à caractère personnel ou, au moins[23], d'avoir connaissance de l'usage qui en est fait[24]. C'est

[22] D.W. SCHARTUM, « Access to Government-Held Information : Challenges and Possibilities », *The Journal of Information Law and Technology*, 1998/1, § 7.1.

[23] Cette nuance est liée au fait que, dans l'e-gouvernement notamment, il y a des situations dans lesquelles le citoyen est obligé de donner ses informations personnelles. C'est le cas, par exemple, des données du Registre national qui sont obligatoirement communiquées et enregistrées à défaut de quoi, le citoyen n'aurait pas d'existence civile.

[24] Dans le même sens, H. BURKERT, « Le jugement du tribunal constitutionnel fédéral allemand sur le recensement démographique », *Droit de l'informatiques et des Télécoms,* 1985,

pourquoi, en l'occurrence, il importe que chaque citoyen puisse avoir une vision claire des bases de données dans lesquelles sont et seront enregistrées les informations qu'il est contraint de donner à l'administration. Dans le même temps, le respect de cet impératif favorise la confiance du citoyen en l'État. Le fait de savoir ce que l'État détient comme données et par quelle administration ces données sont conservées apaise, d'une part, les peurs liées à l'existence d'un État « *Big brother* », qui saurait tout de tout le monde et, d'autre part, les craintes que l'usage des technologies dans le secteur public provoque le développement d'une administration kafkaïenne, c'est-à-dire une administration à ce point opaque et complexe qu'on ne parvient plus à la comprendre et la contrôler[25].

Plus encore, la transparence sous-tend le régime juridique de la protection des données, aujourd'hui organisé par le RGPD. Celui-ci consacre un droit d'accès du citoyen à ses propres données. Ce droit d'accès est particulièrement important car il est la porte d'entrée vers les autres droits consacrés par le RGPD. Par exemple, la personne concernée doit connaitre les données traitées à son sujet pour en vérifier l'exactitude et ensuite exercer son droit à rectification si des erreurs ont été constatées. Ce droit permet également de s'assurer que l'administration ne commet pas d'illégalité dans l'utilisation des données, ce qui serait le cas si ces données étaient utilisées à des fins non autorisées par le RGPD.

Par ailleurs, on ne peut faire fi du droit fondamental à la *transparence administrative*, consacré par l'article 32 de la Constitution et organisé, au niveau fédéral, par loi du 11 avril 1994 relative à la publicité de l'administration[26] et par décrets dans les entités fédérées[27]. Cette dernière impose à l'administration des obligations de publicité active qui consistent à fournir, d'initiative, « une information claire et objective sur l'action des autorités administratives fédérales »[28]. En ce sens, la Charte des services publics impose d'ailleurs clairement aux services publics de recourir aux technologies pour s'adapter aux besoins du public, en affirmant que « par

---

pp. 8 à 16 ; Th. Leonard et Y. Poullet, « Les libertés comme fondement de la protection des données nominatives », *in La vie privée : une liberté parmi les autres ?* (F. Rigaux dir.), Bruxelles, Larcier, 1992, pp. 231 et s. ; R. Leenes et B.-J. Koops, « 'Code' and privacy or how technology is slowly eroding privacy' », in *Coding regulation. Essays on the Normative Role of Information technology* (E. Dommering et L. Asscher dir.), La Haye, TMC Asser Press, 2006, pp. 143 et 144.

[25] Au sujet de ces craintes, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, n^os^ 61 et s.

[26] Loi du 11 avril 1994 relative à la publicité de l'administration.

[27] Décret flamand du 18 mai 1999 relatif à la publicité de l'administration ; décret de la Communauté française du 26 mars 2004 relatif à la publicité de l'administration ; décret de la Communauté germanophone du 16 octobre 1995 relatif à la publicité des documents administratifs.

[28] Art. 2 de la loi du 11 avril 1994.

application de la loi du mutabilité, les services publics doivent s'efforcer de procurer un service adapté aux besoins des utilisateurs, comme aux techniques et moyens disponibles »[29].

Enfin, au-delà de la transparence pour le citoyen désireux de connaître l'usage qui est fait de ses propres données et de pouvoir les corriger le cas échéant, l'impératif de transparence est également nécessaire pour rendre tout à fait effective *l'obligation légale de collecte indirecte des données*. En particulier, il faut que les cours et tribunaux, eux aussi, puissent voir clair sur quel type de donnée est enregistré dans quelle base de données. Il faut, en effet, que les juges puissent vérifier si, dans un cas particulier, la donnée était bien disponible dans le réseau, auquel cas l'administration était obligée de trouver cette donnée par elle-même ou si, dans l'hypothèse où cette donnée n'était pas disponible dans le réseau, l'administration pouvait la collecter directement auprès du citoyen. Une telle vérification suppose que les juges aient eux aussi connaissance des types de données et de leur localisation.

§ 2. Le droit d'accès aux données en pratique

10. Des démarches fastidieuses. Depuis quasiment 20 ans[30], chaque citoyen bénéficie du droit d'accéder aux données que l'administration détient à son sujet. Pourtant, ainsi qu'on a encore pu le constater très récemment[31], nombre d'administrations n'ont jamais été saisies d'une demande d'accès introduite par un citoyen.

Et pour cause. Jusqu'ici, ce droit était très méconnu des citoyens. Gageons du fait que la publicité qui accompagne l'entrée en application du RGPD puisse pallier cette lacune. Mais, même lorsqu'il est connu, ce droit est très peu exercé. Après avoir testé l'exercice de ce droit dans le cadre de nos recherches, on peut raisonnablement penser que son ineffectivité est liée à la lourdeur et à la complexité de sa concrétisation. De toute évidence, la procédure à initier est de nature à décourager un citoyen

[29] Charte de l'utilisateur des services publics du 4 décembre 1992, *M.B.*, 22 janvier 1993, Partie I, Chapitre II, Section 2.

[30] À savoir, depuis l'entrée en vigueur de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, qui consacrait le droit d'accès du citoyen à ses données. Cette loi est aujourd'hui remplacée le RGPD qui organise le même droit en son article 15.

[31] Enquêtes menées auprès d'administrations fédérales, communautaires, régionales et communales en mai 2018 dans le cadre du cours d'E-gouvernement du Master de spécialisation en droit de l'internet (DTIC) organisé à l'Université de Namur.

souhaitant simplement exercer sa curiosité légitime à l'égard du traitement de ses données par l'administration.

En effet, pour connaître les données que détient l'administration à son sujet, ainsi que l'usage qui en est fait, le citoyen doit prendre la peine de rédiger une lettre papier, photocopier le recto et le verso de sa carte d'identité, apposer un timbre qu'il doit lui-même payer, et poster le tout. Il peut introduire sa demande d'accès par courriel, encore faut-il pouvoir authentifier ce courriel[32], ce qui requiert, par exemple, une signature électronique. Une fois la demande introduite, il est contraint de patienter, l'administration disposant d'un mois pour répondre[33].

Par ailleurs, le demandeur d'accès ignore généralement quelle institution détient des données à son sujet. Pour connaître les traitements de ses données, il doit bien souvent introduire sa demande d'accès « à l'aveugle », sans savoir si une réponse intéressante sera fournie.

Notons que pour aider le citoyen à cibler les administrations pertinentes dans le réseau de la sécurité sociale, la Banque-carrefour de la sécurité sociale lui propose de remplir une demander sur papier, en vue d'obtenir un extrait de son « répertoire des références », reprenant les administrations qui ont des données à sujet. Mais le chemin pour accéder à ce document est si difficile que le document est quasi introuvable[34]. Quand bien même il parviendrait à le trouver, le remplir et le renvoyer à la Banque-carrefour, l'extrait qu'il recevra ne reprendra que le nom des administrations, et non les données elles-mêmes. Pour connaître celle-ci, le citoyen doit introduire une demande d'accès auprès de chaque administration visée dans ledit document et patienter…

En somme, comme l'a affirmé le médiateur fédéral dans un dossier relatif à l'utilisation d'une données à caractère personnel erronée dans une décision administrative, « trouver où et comment l'erreur a été commise revient presque à chercher une aiguille dans une botte de foin »[35].

---

[32] Considérant 57 du RGPD.

[33] Art. 12.3 du RGPD.

[34] Pour s'en convaincre, voici un petit exercice : aller sur le site https://www.ksz-bcss.fgov.be/fr et tenter de trouver le document pertinent pour identifier les administrations ayant des données à notre nom. Bonne chance ☺ !

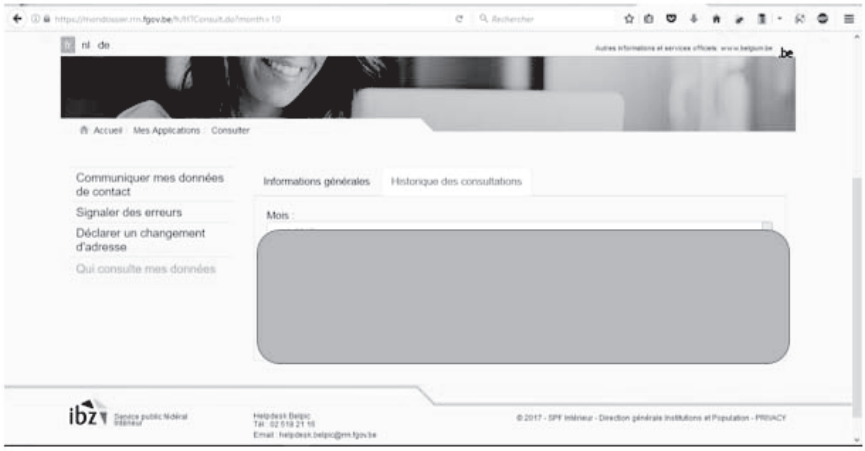
Réponse : aller dans le FAQ, rubrique accès au réseau et aux données,cliquer sur la question « La BCSS enresgitre-t-elle des données à mon sujet et puis-je les consulter », lire le texte, et cliquer sur les mots apparaissant à la fin du texte « "Demande de communication de données à caractère personnel par la Banque Carrefour de la sécurité sociale" ».

[35] Médiateur fédéral, *Rapport annuel 2010*, p. 90.

11. Un ovni : « Mon dossier » au Registre national. Dans le flou entourant la localisation des données au sein de l'administration électronique, on aperçoit un ovni. L'outil « Mon dossier » du Registre national[36].

Cet outil a été créé il y a plus de dix ans par le SPF Intérieur, qui gère le Registre national. Chaque citoyen peut y accéder en ligne. Après s'être identifié avec sa carte d'identité électronique, il accède à un portail qui lui permet de voir l'ensemble de ses données enregistrées au Registre national. Un onglet lui permet de signaler les erreurs affectant ses données, le cas échéant.

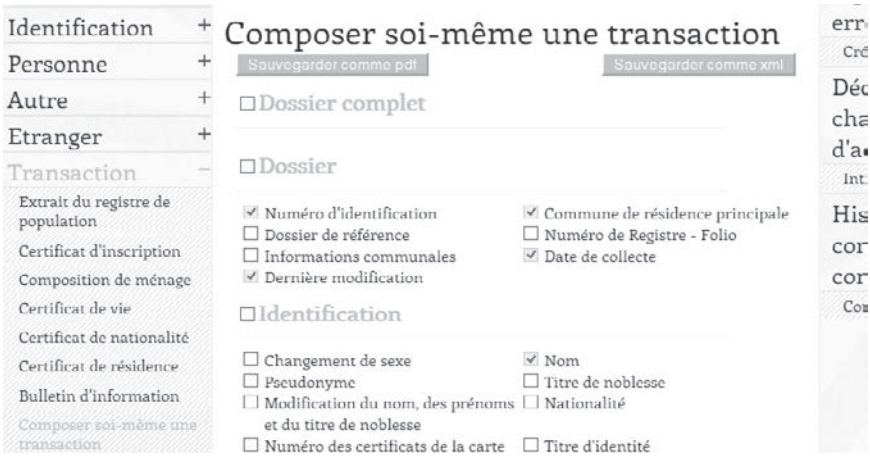
Le citoyen peut aussi cliquer sur l'onglet « Qui consulte mes données », et voir apparaître le nom des institutions s'étant intéressés à lui, dans l'idée qu'il puisse après demander les raisons de telles consultations et en vérifier la légalité.



Extrait du portail « Mon dossier » du Registre national contenant l'onglet « qui consulte mes données »

Enfin, très bon exemple de simplification administrative en pratique, le citoyen peut également obtenir des documents officiels qui nécessitaient jadis un déplacement à la commune. Ces documents sont générés en PDF, assortis de la signature électronique, et ont la même force probante que le même document obtenu à la commune, comme l'affirme l'article 4 de la loi du 8 août 1983 sur le Registre national.

[36] Lien vers l'outil : http://www.ibz.rrn.fgov.be/fr/registre-national/mon-dossier/.



Extrait du portail « Mon dossier » du Registre national, comprenant la liste des documents officiels pouvant être obtenus via cet outil, ainsi que la possibilité de composer soi-même un document en sélectionnant les informations à y faire figurer.

Cet outil est remarquable et devrait être généralisé aux autres bases de données comme nous l'expliquons dans les lignes qui suivent.

§ 3. Les pistes d'amélioration

12. Tenir compte du risque de fracture numérique. On a énoncé précédemment les raisons qui justifient que l'on améliore considérablement la transparence de l'administration électronique.

Respecter cette exigence de transparence ne peut se résumer, pour l'administration, à « dire ce dont elle dispose », de manière brute. C'est un travail qui doit être nourri d'une grande pédagogie dans les explications données et dans l'accès aux outils proposés, compte tenu du nouveau type de fracture numérique qui guette.

Longtemps, la fracture numérique a été entendue comme le fait que certains citoyens étaient exclus du numérique à défaut d'avoir accès à internet et/ou à un ordinateur. On constate aujourd'hui que la fracture numérique se marque de plus en plus à un autre niveau, celui de la compréhension des processus et des enjeux du numérique[37]. Dans ce

[37] À ce sujet, voy. le « Baromètre citoyens 2017. Fracture et inclusion numérique » de l'Agence du numérique https://www.digitalwallonia.be/fr/publications/citoyens2017-inclusion-numerique.

domaine, les citoyens sont inégalitaires, tant cela dépend des aptitudes personnelles, de l'éducation, de la formation.

Il importe donc d'être particulièrement attentif aux inégalités qui existent dans les compétences technologiques de chacun. À dire vrai, le citoyen lambda n'est pas expert en informatique et se sent rapidement dépassé face à des explications techniques. La plupart des citoyens ont donc besoin d'être accompagnés dans la compréhension de ce nouvel environnement.

Dès lors, le souci d'être transparent en fournissant des explications aisément compréhensibles par tout un chacun, et en mettant en place des outils intuitifs et conviviaux, doit recevoir toute l'attention, particulièrement dans le domaine de l'administration électronique qui touche chaque individu, sans exception.

13. Vue d'ensemble et vue individualisée. Ainsi, pour permettre à chacun de bien comprendre l'environnement administratif qui l'entoure, le contexte actuel de l'administration structurée en réseaux amène à travailler la transparence à deux niveaux.

D'une part, il faut organiser une vue d'ensemble claire de l'administration, des types donnés qui y sont enregistrés et des types d'usages qu'on en fait. C'est d'autant plus aisé à mettre en place aujourd'hui que l'administration dispose de tous les outils technologiques permettant de créer un portail internet et d'y faire figurer les documents qu'elle souhaite[38]. Cela permettra notamment d'éclairer les juges dans les dossiers relatifs à l'obligation de collecte indirecte des données et aux citoyens de comprendre l'environnement administratif général qui les entoure.

D'autre part, il faut permettre à chacun d'accéder aisément à ses données, de les vérifier, de signaler des erreurs le cas échéant. Toute personne doit également pouvoir prendre connaissance de l'utilisation qui est faite de ces données, et contester les utilisations abusives, le cas échéant.

14. Vue d'ensemble de l'administration. Une solution serait de créer un portail dédié à l'administration électronique. Celui-ci ferait apparaître un panorama général de la structure administrative offrant suffisamment d'informations sur les outils de traitements de données qui structurent l'administration, ainsi que les échanges de données mis en place.

Le panorama général devrait reprendre l'ensemble des réseaux sectoriels composant l'administration.

[38] Pour de plus amples détails à ce sujet, voy. not. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, n^os^ 377 et s.

En outre, en cliquant sur le réseau sectoriel de son choix, le citoyen devrait voir apparaître la liste des administrations détenant une source authentique de données.

Enfin, en cliquant sur le nom de la source authentique, le type de données enregistrées par celle-ci devrait figurer sur l'écran.

Ce panorama pourrait être complété d'un cadastre des interconnexions. Rappelons-le, l'administration électronique se fonde sur le principe de la collecte unique des données, ce qui entraîne une multiplication des échanges de données entre les administrations.

Ces échanges de données devraient faire l'objet d'une publicité sur le portail internet dédié à l'administration électronique. Cela constituerait une mesure prolongeant, dans l'e-gouvernement, la volonté du législateur d'organiser la publicité active de l'administration, comme en atteste la loi du 11 avril 1994[39], notamment.

À cette fin, le cadastre des interconnexions est un outil particulièrement pertinent. Il peut être défini comme un registre qui répertorie les échanges de données effectués entre les administrations d'un même réseau sectoriel[40]. Un tel outil est d'ailleurs encouragé par la Commission de la protection de la vie privée[41].

15. Vue individualisée de l'administration électronique. Par ailleurs, il faudrait également permettre à chacun d'accéder à une vue individualisée des données détenues à son sujet par l'administration, et de l'utilisation qui en est faite.

Pour ce faire, cela vaudrait la peine de généraliser l'outil « Mon dossier » du Registre national à chaque source authentique de données de l'administration.

---

[39] Art. 2, 1°, de la loi du 11 avril 1994.

[40] Au sujet du cadastre des interconnexions, voy. not. CPVP, avis n° 30/98 du 25 septembre 1998 relatif au registre national, p. 4 ; CPVP, avis n° 28/1999 du 8 septembre 1999 relatif à un avant-projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, p. 6 ; CPVP, avis n° 25/2000 du 10 juillet 2000 relatif au projet d'arrêté royal autorisant l'Intercommunale pour la gestion et la réalisation d'études techniques et économiques, en abrégé I.G.R.E.T.E.C., à utiliser le numéro d'identification du registre national des personnes physiques, p. 4, n° 2 ; CPVP, avis n° 19/2002 du 10 juin 2002 relatif à un projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et modifiant la loi d du 8 août 1983 organisant un Registre national des personnes physiques (…), p. 10, n° 18.

[41] CPVP, avis n° 23/2008 du 11 juin 2008 relatif à un avant-projet de loi portant création de la source authentique des données relatives aux véhicules, p. 33, n° 108.

Concrètement, en consultant le portail internet dédié à l'administration électronique, le citoyen devrait pouvoir s'identifier avec sa carte d'identité électronique et voir apparaître la liste de toutes les sources authentiques de données qui contiennent des données à son sujet. En cliquant dessus, il pourrait consulter ces données, comme il peut le faire pour le Registre national.

Il faudrait également mettre en place un « audit trail » c'est-à-dire un outil permettant de tracer les échanges de données entre les différentes administrations. De telles informations peuvent être très intéressantes lorsqu'il s'agit, par exemple, de trouver la source d'une erreur affectant une donnée et de prévenir chaque institution l'ayant utilisée[42].

Ce sont des pistes pour lesquelles nous plaidons depuis longtemps déjà. À la faveur de l'entrée en application du RGPD, notamment, la situation dans ce domaine a l'air de progresser depuis peu. Récemment, l'Office de la transformation digitale du SPF Stratégie et Appui a créé un portail internet dénommé www.passezaudigital.be. On y annonce la création d'un portail web pour les administrations. L'explication, encore fort vague, affirme qu'il s'agit d'« une application qui permet aux différentes institutions fédérales d'enregistrer les données comme l'exige le RGPD ». On y annonce également que « par la suite, les citoyens européens pourront également consulter ce portail web pour voir les données dont dispose le gouvernement à leur sujet, à quelles fins ces données sont utilisées et de quelle manière ils peuvent faire exercer leurs droits, par exemple le droit à l'oubli ou le droit à la portabilité des données ». Espérons qu'il s'agisse là d'une réelle mesure de transparence et d'information au bénéficie des citoyens et qu'elle sera effectivement suivie en pratique.

Conclusions

À l'heure actuelle, le numérique apparaît tant comme une opportunité qu'une menace pour le citoyen.

C'est une *opportunité* en ce que le développement de l'administration électronique pousse à évaluer et repenser la relation entre le citoyen et l'administration. En filigrane de ces réflexions, apparaît l'envie de supprimer les sources d'agacement mutuel liées principalement à la paperasserie, à la sempiternelle communication des mêmes informations à chaque

[42] Pour plus de détails à propos de la mise en place d'une vue individualisée de l'administration, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, nos 396 et s.

démarche administrative, aux files d'attente. Le numérique allège considérablement ces tâches, tant pour l'administration que le citoyen. De toute évidence, les premières expériences de simplification administrative sont prometteuses et notre modèle d'administration électronique, inédit, est à encourager moyennant certaines balises.

Si des balises sont nécessaires, c'est parce que le numérique est aussi une *menace* pour le citoyen, perdu par rapport à la complexité et à l'opacité de l'administration électronique. À cet égard, on a souligné l'importance de se concentrer sur l'amélioration de la transparence des outils, en faisant preuve d'efficacité et de pédagogie pour que chacun puisse voir, comprendre et contrôler l'usage de ses données dans l'administration. À défaut, on prendrait le risque de créer une nouvelle fracture numérique, non plus dans l'accès à internet, mais dans la compréhension du fonctionnement de l'administration et de la relation que nous entretenons avec elle.

Ces préoccupations doivent être rencontrées, non seulement pour répondre à l'impératif de transparence fondé sur des justifications constitutionnelles et légales, mais aussi, plus largement, pour maintenir la confiance du citoyen en l'État. C'est là, probablement, le défi majeur à relever pour assurer le succès de notre administration électronique à long terme.

***